EXHIBIT 1

UNITED STATES DISTRICT COURT

DISTRICT OF MARYLAND

COTTON PATCH CAFÉ, INC., 4825 W. Royal Land Irving, Texas 75063 Plaintiff, v. MICROS SYSTEMS, INC., 7031 Columbia Gateway Drive Columbia, Maryland 21046 Defendant.	CIVIL ACTON NO. 1:09-CV-03242-MJG

First Supplemental Expert Report of Roger Nebel

I. Qualifications

1. I currently serve as Managing Director for Cyber Security at Defense Group, Inc. ("DGI") in Washington, D.C. My business unit serves federal, state, and local government cyber security clients. In addition, I lead the commercial information security and subject matter expert services practices at DGI. I also serve as the chair of the Cyber Security Executive Committee at DGI and as the Chief Information Security Officer. I have over 30 years experience in the Information Technology, Software, Internet, and Information Security fields. I am intimately familiar with developing, testing, implementing, and auditing software-based systems and, specifically, Internet-facing applications. I am familiar with the risks and appropriate safeguards[1] involved with Internet-facing systems such as the one at issue in this matter. I have investigated many data security breaches, including payment card breaches at retailers who were running the Micros Point of Sale ("POS") system at the heart of this matter. DGI was retained by counsel on behalf of Plaintiff at an hourly rate of $325. Payment is not contingent on my opinions. A recent CV is attached as Exhibit A.

2. Prior to my role at DGI, I served as strategic security national practice leader in the Technology sector of FTI Consulting, a leading computer forensics and electronic evidence firm. I am very familiar with developing, testing, implementing, and auditing software-based systems, and specifically with the technology used in POS systems that process electronic payment cards. I have personally developed information security and privacy standards based on industry best practices and conducted hundreds

[1] Throughout this document I may interchangeably refer to controls, countermeasures, and safeguards. The various credit card security standards discussed in this report also interchangeably use these terms in the same way. They are functionally equivalent concepts and essentially mean any measure taken to reduce risk — whether by people, process, or technology — or in some combination. Similarly, a compensating control supplements or replaces one or more weak controls.

of audits using many standards, including the Payment Card Industry Data Security Standard ("PCI DSS"), its antecedents, and the related payment applications standards which govern the information security in this matter. I am familiar with how software and POS systems such as those provided by Micros are specified, developed, tested, accepted, deployed, maintained, secured, and operated in the field by retail organizations such as Cotton Patch Cafe. I am very familiar with the examination of complex software systems, technology outsourcing arrangements, and related disputes, and have personally written audit reports, expert opinions, and provided testimony based on similar examinations.

3. For the first two decades of my career I developed, maintained, and tested complex systems and software applications for the United States Federal Government as a contractor supporting worldwide Intelligence, Command and Control, and Special Operations missions. This experience includes substantial work designing operational security controls to provide authorized access to sensitive information and to protect sensitive information against unauthorized access. I also have substantial experience with the art and science of conducting assessments and audits of those controls.

4. In July of 1996, a colleague and I formed a security consulting business that we subsequently sold to HomeCom Communications where, as an officer and director, I led security consulting efforts for major financial institutions such as Citibank and Pershing, supported acquisition due diligence, and conducted security audit activities in the Internet banking space. In 1999, we sold the security consulting business to iDefense.

5. While at iDefense as the Chief Technology Officer (CTO) from 1999 to 2001, I participated in, and then led the design, building and operational deployment of a

commercial intelligence delivery system for Internet security vulnerability information.[2] I contributed as a subject matter expert in the development and delivery of complex vulnerability and exploit knowledge bases which continue in operation to this day at Verisign.[3] In addition, I co-authored and was a co-inventor on the iDefense patent application.[4] From 2001 to 2004, I was Vice President of Services at TruSecure where I founded the application security consulting practice in addition to managing the defined security program which, over its lifetime, has had over 1,000 customers including numerous Internet banks, retail merchants, and payment processing services companies such as the well-known ExxonMobil Speedpass system that can link to many consumer credit cards. At iDefense and then at TruSecure (where we acquired the Vigilinx vulnerability tracking database service), we tracked tens of thousands of software security bugs and the vendor responses and fixes for those bugs. I continued in this field of work with security at FTI where, as a Visa CISP and then as a PCI DSS certified assessor, I led teams that audited and reported on merchants and service providers with the PCI DSS requirements for protecting sensitive Card Holder Data ("CHD"). In addition, I was also certified to conduct audits of payment applications under Visa's Payment Application Best Practices ("PABP") and later under the payment card industry's Payment Applications Data Security Standard ("PA-DSS").

6. Over the most recent decade I have designed, built, or audited hundreds of applications that provide access to sensitive information including banking, securities trading, payment card processing, and retail operations. I have investigated data breaches

---

[2] http://www.idefense.com

[3] Verisign acquires iDefense, http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_031054.html

[4] iDefense patent application, http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=31&f=G&l=50&co1=AND&d=PG01&s1=nebel.IN.&OS=IN/nebel&RS=IN/nebel

and advised hundreds of firms on the issues of security and their obligations for protecting privacy. I have analyzed, lectured, reported, or testified on, among other topics, the subjects of Internet security, credit card security, and digital intellectual property at copyright royalty board hearings in litigation, arbitration, and in complex software and technology disputes. I have served as an independent consultant, conducted in-depth technical analyses, and personally led reporting on settlements before the SEC, NYSE, and FTC involving breach of duty and other regulatory violations, including credit card fraud and data breaches. My trial and deposition testimony over the past four years is attached as Exhibit B.

7. I am a founding Adjunct Professor at the University of Virginia in the graduate Information Security Management program where, since 2001, I have developed curricula and or taught each of the six core courses and one elective course. Beginning in the fall of 2010, I have been the lead instructor in the new graduate Information Assurance track in the graduate school of professional studies at Georgetown University.

8. As an executive at five commercial companies in the past decade, I have become familiar with the generally accepted industry standards for information security, data privacy, and the regulatory and contractual standards for information security and data privacy under those regimes. At TruSecure, I delivered or oversaw security audits and assessments for hundreds of organizations as part of their security compliance due diligence. I also oversaw contracts under which TruSecure provided preferred third-party security audit services for major service providers in the financial institutions marketplace, including companies such as Fiserv,[5] Pershing, and Equifax.

---

[5] Beginning in 1997, I developed one of the first Internet banking security audit standards frameworks to be accepted by the interagency financial institution regulators (FFIEC, OCC, FDIC, OTS, NCUA). This began what was a decade-long relationship where Fiserv uses that framework for all of its regulated Internet systems.

9. I have been a Qualified Security Professional under the auspices of the Payment Card Industry ("PCI") Security Standards Organization. I have been a Qualified Payment Applications Security Professional under the rules of Visa International and PCI. In these roles I was responsible for assessing the security of payment card information and the applications that process sensitive payment card information. On March 12, 2008 I presented to over 70 Office of Thrift Supervision ("OTS") regulators on the subject of financial fraud technology trends with an emphasis on payment card fraud. I was retained for over a year by a professional sports league client to work for a good set of rules under the Unlawful Internet Gambling Enforcement Act which regulates how banks and electronic payment service providers are to detect and block electronic payments to offshore gambling enterprises by U.S. citizens.

10. I am both an internationally recognized Certified Information Systems Auditor and a Certified Information Systems Security Professional — essentially holding licenses for the past decade to audit and render opinions on the management, operation, and failures of complex security technologies. I have agreed to certain standards of ethical conduct to continue to hold these professional certifications and must meet a minimum number of Continuing Professional Education (CPE) hours each year.

II. Assignment

11. I was asked by counsel for Cotton Patch to analyze the facts in this matter in light of the relevant payment card industry standards and practices, and the relationships and data security obligations of the various parties involved in this lawsuit. In approaching my assignment, I begin by identifying and explaining the relevant data security standards, how they apply for merchants and payment application vendors, and how they are generally implemented by those parties. I then explain the relationships that exist between the various credit card security parties. I then lay out a timeline of material events leading up to this lawsuit and analyze how Micros was aware of both its data security obligations and the vulnerabilities present in its products. Finally, I render opinions using my professional judgment as an expert in this field.[6]

12. In summary, Micros was fully aware of both relevant data security standards and the many security vulnerabilities present in the Micros system sold to Cotton Patch and serviced by Micros over several years at Cotton Patch's Nacogdoches, Texas location. Micros was not only aware of vulnerabilities in the Micros system, and specifically at the Nacogdoches location, but Micros represented to Cotton Patch that its POS system complied with the prevailing data security standards, a representation that Cotton Patch relied upon. Micros failed to fulfill its obligation to Cotton Patch by failing to maintain Cotton Patch's POS system in a manner compliant with relevant data security standards including, among other requirements, prohibitions on the storage of full track data, requirements to encrypt sensitive CHD, and requirements barring the use of default and non-unique (i.e., common and shared) userids and vendor-supplied passwords. Micros also failed to adequately disclose these vulnerabilities to Cotton Patch.

---

[6] A list of the documents I received from counsel for Cotton Patch is provided in Exhibit N.

III. Factual Analysis

A. The Credit Card Security Standards

13. In general, the credit card security standards discussed below are the result of evolutionary changes within the payment card industry that have served to reduce fraud by increasing security. Each evolution has been accompanied by a tremendous communications effort by Visa, MasterCard, American Express, Discover, PCI, member banks, and others within the industry.[7] The credit card security standards are based on well-accepted security concepts that include layered controls, sometimes referred to as defense-in-depth, and upon a well-known risk formula that is often expressed as:

Risk = (Threat x Vulnerability) – Countermeasures

Most security practitioners (and mathematicians) would agree that if either Threat or Vulnerability is zero (or mathematically near zero), then Risk is essentially zero (or mathematically near zero). Thus, the credit card security standards attempt to push Vulnerability towards zero by prohibiting the storage of full magnetic stripe track data, by requiring encryption of any sensitive CHD that is stored, and by prohibiting the use of default, common, or shared userids.[8] If the Micros payment application had not stored full magnetic stripe track data, had encrypted sensitive CHD, and had not used common and shared userids, the odds of a compromise would have been pushed towards near zero.

14. Visa Cardholder Information Security Program ("CISP"). Launched by Visa in April 2000, the CISP, which became mandatory in June 2001, was intended to reduce fraud by improving and standardizing how the various parties in a credit card

---

[7] In April 2007 I was instrumental in organizing and presenting at an industry symposium in New York that was attended by Visa, major merchants in the Northeast, and several PCI interested vendors. *See* Exhibit E for copies of the presentations made that day in no specific order.

[8] For further information, see the discussion of statutory breach notification requirements later in this same section of the report. The vast majority of those statutes do not require a notification if the data was encrypted because strong encryption (such as 3DES) essentially reduces Vulnerability to near zero.

transaction were to identify and reduce risk. In November 2000, Visa published the Account Information Security Standards Manual which prohibits use of default userids and passwords and requires protection of magnetic stripe data (i.e., the data embedded on the magnetic stripe on the back of a credit card). *See* Exhibit L at pages 4-1, 4-2, and 4-12. By 2004 the CISP had evolved to include assessment standards. Version 2.3 of the CISP standard, dated March 24, 2004, clearly prohibits the storage of full magnetic stripe data. *See* Exhibit C at 10 Requirement 3.4. This standard also prohibits the use of default userids and passwords, and requires that any sensitive CHD be protected by strong encryption (i.e., 3DES) or other means such as obfuscation. *See* Exhibit C at 11 Requirement 3.6; *id.* 22 Requirement 8.

15. Visa Payment Applications Best Practices ("PABP"). In 2004, Visa launched the PABP, a set of software system life cycle best practices for payment application vendors to follow. *See* Exhibit J. Version 1.2 of the PABP was issued on September 13, 2005, and prohibited the storage of full magnetic stripe or track data as a further way to reduce fraud by improving the security in payment applications software that is often purchased from vendors, like Micros, who specialize in POS applications. *See* Exhibit D at 5-6 Requirement 1. The PABP "suggests that vendors document the configuration specifics . . . and advise their customers that the application has to be configured as stated." *Id.* at 16. This was generally referred to as the Secure Configuration Guide. *See* Exhibit D at 16, fn. B. This guide also required unique (i.e., not default or common) userids and passwords for administrative access, *see* Exhibit D at 8, Section 3.1, and that sensitive CHD be rendered unreadable "anywhere it is stored," *see* Exhibit D at 7, Requirement 2.2.

16. Payment Card Industry Data Security Standard ("PCI DSS"). Visa's CISP and the equivalent programs of MasterCard, American Express, and Discover Card, were merged beginning in 2004 and after a phase-in period, mandated by all of the card brands in April 2008. The card brands continued to manage their own respective compliance requirements (what reporting was required, how often, etc.), but with all brands using the new unified PCI standards. Version 1.0 of the PCI DSS is attached as Exhibit H. Requirement 3.2 of Version 1 of the PCI DSS clearly prohibits the storage of full magnetic stripe track data. *See* Exhibit H at 4. Requirement 2 prohibits the use of vendor-supplied (i.e., default) userids and passwords. *Id.* at 3. Requirement 3.4 also requires that any sensitive CHD be rendered unreadable "anywhere it is stored." *Id.* at 4.

17. Payment Application Data Security Standard ("PA-DSS"). Visa and the other card brands agreed to merge the PABP into the PCI standards organization and renamed it PA-DSS Version 1.1 beginning in April 2008. *See* Exhibit K. A phase-in period covered new and existing payment applications on differing schedules. Requirement 1 of the PA-DSS standard clearly prohibits the storage of full magnetic stripe track data. *See* Exhibit K at 1-5. Requirement 3 clearly prohibits the use of default and common accounts. *Id.* at 8-9. Requirement 2.3 mandates that the Primary Account number (PAN) be rendered unreadable "anywhere it is stored." *Id.* at 6-7.

18. In addition to the credit card security standards that are designed to reduce fraud, there are other Visa and PCI standards,[9] as well as a statutory and regulatory regime that applies to financial institutions and those organizations that possess certain Personally Identifiable Information ("PII") implicated in identity theft such as social

[9] See, for example, pcisecuritystandards.org for a list of the standards they currently oversee.

security numbers, bank account numbers, and credit card numbers,[10] to name a few. For example, certain states have statutory requirements to notify consumers following a breach of payment card information. Under the majority of those state statutes there is no requirement to notify if the data had been strongly encrypted. Similarly, banks have a duty under the Graham-Leach-Bliley Act ("GLBA"), the Fair Credit Reporting Act ("FCRA"), and FACTA, among other laws and rules, to protect PII and report apparent breaches.

B. Common Industry Practices

19. It is common in the retail payment card industry — which includes banks, merchants, payment application vendors, and service providers — for smaller, relatively unsophisticated merchants such as Cotton Patch to outsource much or all of their Information Technology (IT) service provision to a vendor such as Micros[11]. This outsourcing can be as simple as purchasing products and employing full-service call centers. Cotton Patch's practice of "buying as it goes" from Micros is very common. Indeed, the original sales contract between Cotton Patch and Micros relating to the Nacogdoches restaurant reflects this on-going relationship. *See* CP000205-213. Examples of this on-going relationship include the marketing data pull in 2004 and the server replacement in 2006 discussed later in this report. *See* M000290, M000305-6, and M000187-191.

20. Cotton Patch, as a merchant restaurant, specializes in food service for consumers, some of whom desire to pay with a credit card. Micros, as a payment application vendor, specializes in Point of Sale products and services for the food service

---

[10] An informative article regarding the topic of credit card breaches and identity-related crime appears at https://www.pcisecuritystandards.org/pdfs/DataBreachesArticle.pdf, which is attached as Exhibit G.

[11] Micros represented to Cotton Patch that it provided what was effectively an outsourced, turn-key system. *See* Deposition of Alan Mann at page 68 lines 19-25.

industry niche that Cotton Patch occupies. Cotton Patch is not in the IT provision business and relied upon Micros to fill that role. Micros, as a payment application vendor to the food service industry, is both knowledgeable about the needs of the industry and experienced in providing products and services that fit that need.

21. Cotton Patch necessarily depended upon Micros to understand the needs of Cotton Patch, including the need for a secure and ultimately PCI DSS compliant product. Among other things, Micros was in the best position to ensure that the Micros POS system at the Cotton Patch Nacogdoches location: a) did not store full track data post-authorization, b) rendered sensitive CHD unreadable "anywhere it was stored", and c) did not use default or common userids and passwords.

22. Micros represented to Cotton Patch that this reliance was trustworthy. Cotton Patch was led to believe that Micros was handling the compliance needs of Cotton Patch, and in some cases this reliance was satisfied. However, as discussed below, Micros was aware of critical security deficiencies in the Micros products at the Nacogdoches location that Micros failed to adequately communicate to Cotton Patch. Specifically, Micros was fully aware that the POS application that Micros sold to Cotton Patch and that was running at the Cotton Patch Nacogdoches location did not encrypt sensitive CHD. *See* Deposition of Stephen Freitag at 26:12-18, 36:20-38:11, 66:18-67:10, 72:6-13; Deposition of Scott Shipferling 151:9-20. In addition, Micros was aware, or should have been aware, that the Micros POS system was storing full magnetic stripe track data in violation of the various credit card security standards. Micros was also aware, or should have been aware, that sensitive CHD was not being "rendered unreadable anywhere it is stored." Finally, Micros created and continued to use common usersids and passwords to remotely access the Nacogdoches server. Had Micros

addressed these critical vulnerabilities in its POS system, there would have been a significant reduction in the risk of a compromise at the Cotton Patch Nacogdoches location. Failing to communicate or remediate these deficiencies is not a common practice, and these deficiencies were identified by a third-party as the likely cause of an alleged data security breach.

C. The Credit Card Security Parties, Relationships, and Obligations

23. Cotton Patch Café is a restaurant chain that operates primarily in the State of Texas. Micros Systems is a vendor of point of sale software, systems and services that is headquartered in Columbia, Maryland with a sales and services office in Dallas, Texas. Cotton Patch contracted with Micros in 2001 for on-line POS systems to be installed at Cotton Patch's Nacogdoches location, and has continued to contract with Micros throughout the alleged breach and even until today. Pursuant to these contracts, Micros provides software, hardware, and maintenance and upgrade services to Cotton Patch for the Nacogdoches restaurant.

24. It is important to understand how the Payment Card Industry is structured and operates in order to appreciate where key knowledge and obligations lie with respect to securing sensitive data. Visa and MasterCard are each member bank associations — their members are the banks that issue credit cards (Issuers) and process transactions for their merchant customers (Acquirers).[12] Often banks also own and operate service providers and transaction processing firms. For simplicity, when I refer to Visa in this report, unless I state otherwise I am including MasterCard and the two other card brands (American Express and Discover Card), as they all operate in a similar fashion, and now

---

[12] American Express and Discover Card are stand-alone corporations that operate as both acquirer and issuer.

use the same information security standards through the Payment Card Industry Security Standards Council.

25. RBS Lynk[13] was a payment card transaction processor with whom Cotton Patch contracted to purchase certain payment card transaction processing services. RBS is a bank that is both an issuer of cards and an acquirer of transactions. RBS owned and operated RBS Lynk, a payment card transaction processor. Responsibility for reducing fraud is ultimately shared among the card brands, banks, merchants, service providers, and payment application vendors, with each entity bearing certain obligations. The only contractual relationship that exists for Micros[14] is with its retail customers — in this case, Cotton Patch. Since Visa does not have a contractual relationship with payment application vendors such as Micros, Visa cannot directly mandate them to comply. Visa must rely on other mechanisms, such as audit procedures whereby vendor product versions become "validated" as compliant with PABP and PA-DSS standards. While this matter is not a contractual dispute per se, one cannot analyze these events without being aware of relevant contractual obligations and relationships, and more importantly, who possesses the critical knowledge necessary to comply with the applicable standards and avoid a breach.

26. In this collaborative environment, where there are overlapping sets of standards and obligations, adequate and effective communication of issues is absolutely necessary in order for a relatively unsophisticated merchant such as Cotton Patch to

---

[13] RBS Lynk (formerly Lynk Systems) is now known as WorldPay.

[14] Payment vendors may also contract separately with qualified industry firms to obtain PABP and PA-DSS compliance statements for their payment applications with the PABP or PA-DSS requirements. In that case, the industry firm doing the assessment has a contractual obligation to Visa or PCI, but the application vendor does not, beyond an attestation of full disclosure to the compliance assessor.

remain knowledgeable about vulnerabilities[15] in payment applications like the Micros POS system that Cotton Patch was using at the time of the alleged breach. It is a common industry practice for small retailers like Cotton Patch to rely upon payment application vendors such as Micros. In the payment card application industry it is also common for vendors like Micros to find out about vulnerabilities in their applications from Visa and other customer merchants. It is also common for vendors such as Micros to become aware of compliance standards and for their products to come into compliance as a natural part of market forces.

D. Timeline and Events Relevant to Cotton Patch Nacogdoches

27. I spoke directly with Cotton Patch employees Alan Mann and Duane Herring, and Cotton Patch President Larry Marshall, to ascertain the relevant facts surrounding the history of Cotton Patch's relationship with Micros and to gain an understanding of the evolution of the POS system at the Nacogdoches, Texas location where the alleged breach was reported to have occurred.

28. Based on these interviews, it is my understanding that Cotton Patch purchased an on-line version of Micros "RES" (Micros' POS system for restaurants) for Nacogdoches in 2001, and maintained an on-going "per-call" contractual / invoice relationship with Micros for upgrades, maintenance, trouble-shooting, and other services. This type of relationship is a typical way for small merchants to conduct business. Cotton Patch would call or email Micros and Micros would respond with a service call, either on-site or remotely. In some cases, Micros did not invoice Cotton Patch for these calls.[16]

---

[15] As indicated earlier, I have substantial experience with the challenges of keeping up with security vulnerability information for all organizations. Cotton Patch relied on Micros to keep them informed and secure.

[16] Interview with Alan Mann on June 22, 2010.

29. Throughout the parties' relationship, Micros maintained control over the RES system installed at Cotton Patch's Nacogdoches restaurant. Indeed, Micros directed Cotton Patch employee Alan Mann from 2001 to 2007 to "stay out" of the operational system.[17] As the relationship went on, Micros became aware of multiple vulnerabilities in the Micros RES system, and specifically with vulnerabilities in the Micros RES system running and maintained by Micros at Cotton Patch's Nacogdoches location. Despite this knowledge, Micros failed to adequately communicate information to Cotton Patch about the many deficiencies in the RES POS system until it was too late to prevent a breach.

30. Payment application vendors such as Micros become aware through various means of requirements for their merchant customers to be compliant with CISP, PCI DSS, PABP, and PA-DSS (the "Credit Card Security Standards" or "Standards").[18] Micros was well aware of Credit Card Security Standards compliance requirements as far back as October 2003[19] and their key role in this compliance, because Micros authored at least three documents on this topic, all of which are analyzed in this event timeline. Micros also dedicated resources to complying with those requirements in order to successfully obtain compliance listing from Visa of their many payment applications. *See, e.g.*, Exhibit F.[20]

31. In 2001, Cotton Patch and Micros executed a sales contract for the purchase of software, services, and equipment for the Nacogdoches location. *See* CP000205-213. The sales contract contains certain terms and conditions. *See*

---

[17] *Id.*; *See also* Deposition of Alan Mann at 50:9-13, 52:22-25, 54:4-18; Deposition of Scott Shipferling at 51:4-12, 156:16-157:6; Deposition of Ryan Ritter at 116:2-25, 174:24-175:12; Deposition of Duane Herring at 172:22-174:1.

[18] These standards are detailed later in this report.

[19] *See* Deposition of Stephen Freitag at 58:15-59:1; M002482-2484; M001744-51; M000490-91; M000864-72.

[20] Interestingly, no Micros products appear in Exhibit M, dated November 14, 2005 in apparent contradiction with the claims in M000280.

CP000208-9. Paragraph 16 of the sales contract contains a standard grant of software license under which Micros retains the full ownership and control of the Micros software and prohibits Cotton Patch from making any modifications. The behavior of the parties supports this as Cotton Patch continued to rely upon Micros for modifications as necessary. Paragraph 16 states, "Micros will not provide software support or upgrades to Customer unless the Products include help desk support service and/or a software enhancement license." *Id.* One of the items purchased was "HELPDESK ONE YEAR, 7x24, 1-800 HELP DESK $930.00". *Id.* at CP000207. This appears to be the initial purchase of help desk support service mentioned in paragraph 16. Based upon the behavior of the parties over the years whereby Cotton Patch would call Micros for support and Micros would provide that support to Cotton Patch, it is clear that Cotton Patch continued to rely on Micros in the ensuing years for software and system support and upgrades, albeit on a per-call invoice basis. Thus Micros and Cotton Patch continued to have mutual obligations, the parties' behavior was consistent with those obligations, and Cotton Patch in turn relied on that continuing relationship and obligation.

32. In 2003, Micros began to internally recommend that Cotton Patch move to Digital Subscriber Line (DSL) service, a form of always-on broadband Internet connectivity. *See* M000307. Micros subsequently introduced high-speed Internet processing. *See* Deposition of Scott Shipferling at 100:5-13. This persistent Internet connectivity greatly contributed to the increasingly dangerous exposure of the many Micros vulnerabilities at the Cotton Patch Nacogdoches location. Indeed, absent this single change, the vulnerability surface of the Micros system would have remained very small at the Cotton Patch Nacogdoches location and no compromise may have ever occurred. Switching to DSL did speed up authorization at the restaurant, but just as

importantly, it significantly eased Micro's remote maintenance as software updates could more efficiently be pushed over the Internet on broadband rather than the slower dial-up connection that previously existed.

33. In 2004, Micros is clearly seen as controlling access to the Cotton Patch POS systems when they ask for permission to add a new, shared user for some reporting requirements. Micros, not Cotton Patch, directly controls new users accessing the system over the Internet and Cotton Patch simply approves what Micros is asking for. *See* M000290. It is also important to understand that in 2004, shared users were not allowed under CISP, and they are still not allowed under PCI DSS. *See, e.g.*, Exhibit C at 19-22 Section 7 (indicating that a unique ID should be assigned to each person with computer access); Exhibit D at 8, Section 3.2 of the Visa PABP.

34. On September 14, 2004 Visa published the Payment Applications Best Practices (PABP) Version 1.0.[21] In this document Visa indicates on page 1 that the payment application "must not store full magnetic strip or CVV2 data after authorization is complete." *See* Exhibit J at 1, Best Practice 1. On page 2 Visa writes "Internet applications should not store cardholder data on Internet-accessible systems" and should "[f]acilitate secure remote access . . . ." *Id.* at 2, Best Practices 9 & 11. PABP also provides that sensitive CHD should be protected with strong encryption. *See* Exhibit J at 1, Best Practice 2. According to the Trustwave report issued after the data security breach at Cotton Patch's Nacogdoches restaurant in response to the breach, *see* M000140-164, the Micros application at Nacogdoches during the time leading up to the alleged compromise (and as late as November 2007, *See* M000156) was storing full magnetic stripe data, and remote access via PCAnywhere was not secure because there

[21] While it is sometimes seen that the first versions of a standard are indicated with numbers less than 1.0, it is typical that Version 1.0 is the first production release of a standard.

were default and or common or shared userids and passwords in use by Micros to facilitate support. *See* M000146. Both of these vulnerabilities were violations of the existing PABP standards of which Micros was well-aware.

35. On November 7, 2005 Micros authored a document addressed "Dear Valued Customer" that detailed Visa CISP requirements to secure the remote management program called PCAnywhere by changing generic (i.e., default, common, or shared) userids and passwords.[22] *See* M000282. *See also* Deposition Exhibit 27 (December 27, 2005 version of the letter). This is because generic and default userids and passwords are well known to miscreant attackers and are the source of many breaches. Indeed, Trustwave indicates this as an issue with the Nacogdoches location in their report. *See* M000146 at item 2 in Table 1-2. The Micros document goes on to read: "These [userids] will be needed by MICROS anytime you require support on your MICROS system. Otherwise, we will be unable to access your system remotely." *See* M000282. Micros was aware of this default, insecure configuration because it used one or more of these userids and passwords to access the Cotton Patch Nacogdoches location for maintenance and support.[23] Interviews with Cotton Patch employees revealed that Cotton Patch, when calling the Micros call center in Maryland for support, did not have to communicate the userid and password for remote access because "Micros already knew the userid and password to use for remote access to all our locations."[24] In similar breach investigations I have noted common and default userids and passwords as an

---

[22] Apparently this November 2005 Micros guidance on PCAnywhere contradicts earlier Micros Remote Access/Customer Support Policy as early as 2003 which states that PC Anywhere "...[s]hould only be used inside a secure connection such as VPN [sic]..." because the Cotton Patch Nacogdoches location, as implemented by Micros, did not have such a VPN. *See* M008986-99.

[23] *See e. g.*, Deposition of Clayton Starkweather at 79:16-80:12, 124:11-127:8; Deposition of David Williams at 55:20-56:10; Deposition of Stephen Freitag at 51:12-52:20; Deposition of Robert Gibson at 37:13-40:13. *See also*, M002083; M000430-31; M004378-84; M004387; M000290.

[24] Interview with Alan Mann on June 22, 2010.

endemic issue at other food service locations using Micros POS products. Cotton Patch was not aware that this continuing practice was in violation of data security standards of which Micros was aware, and Cotton Patch could not have fixed the common userids and passwords because these were implemented[25] and maintained by Micros.

36. In this same November 7, 2005 document, Micros is seen to be aware of and addressing some of the secure remote access requirements of Visa seen in Exhibit J (which also refers to the unique userid requirement referenced in Exhibit C). In addition to speaking with Cotton Patch employees, I reviewed Micros invoices for continuing service calls. I also analyzed some relevant emails provided by Micros. I am informed by Cotton Patch employees that they relied exclusively upon Micros for software, hardware, trouble shooting, and service calls. It is clear to me that this reliance occurred over a long period of time — from at least 2001 and continuing even today.

37. On February 10, 2006 Micros authored a document addressed "Dear MICROS Customer" and containing the legend at the top "IMPORTANT LEGAL NOTICE." *See* M000280. This document states: "When the new Association [PABP] guidelines were announced, which prohibited the long-accepted and approved practice of storing track data, MICROS implemented changes to **all** of its PMS/POS applications to prevent the storage of full magnetic stripe strip data. **These enhanced MICROS products have been made available to all MICROS customers since March 2004**, subject to standard upgrade charges . . .[a]ttached is the status report for the MICROS products."[26] *See* M000280[27] (emphasis added). Based on my conversations with Cotton

---

[25] *See* M009017 which clearly shows Micros as the implementer of the common userids and passwords at Cotton Patch Nacogdoches on 3/17/2006.

[26] Note that the Micros RES 3.2 Service Pack 7 Hot Fix 5 version first appears to be a Visa PABP validated version on 12/31/2006 – apparently contradicting the statement that all applications had been available in March 2004. See Exhibit F. The Cotton Patch Nacogdoches location was upgraded to RES 3.2 SP7 HF5 on or about September 5, 2007 after Cotton Patch was notified of a potential breach based on CPP.

Patch employees, I understand that Cotton Patch was not told of the availability of PCI compliant versions of Micros beginning in March 2004, or at any subsequent date prior to the alleged breach, nor to eliminate full track data that the Micros POS application had been storing at the Cotton Patch Nacogdoches location. Based on these same conversations, I further understand that Cotton Patch did receive this document prior to the CPP notice, nor did Micros adequately follow-up with Cotton Patch regarding the March 2004 upgrade or the February 2006 document.

38. In 2006 in a series of internal emails, Micros is aware that the Nacogdoches site is, or will be, running a non-PCI-compliant version of the Micros software on insecure platforms. *See* M000305-6. Micros is also seen to be discussing the potential for an upgrade from RES version 3.1 to 3.2. *Id.* This is critical because at this point in 2006, Micros performed a server replacement at Nacogdoches due to a hard drive crash.[28] This hard drive crash and eventual system replacement would appear to be the event that led to the internal Micros emails seen at M000305-6. At this point in time, Micros is fully aware of the compliance status of RES versions 3.1 and 3.2 and that the Nacogdoches location is running the non-compliant RES version 3.1. Regardless, version 3.2 service pack 6 hot fix 3 was also not compliant at the time. *See* Deposition of Stephen Freitag at 66:25-68:10.

39. On or about March of 2006, one of the Cotton Patch owners, Larry Marshall, had one or more conversations with one or more Micros employees on the topic of masking credit card numbers after Mr. Marshall had seen or heard a news story on the same topic. Cotton Patch asked for, and obtained, an oral representation from

---

[27] I also understand that Micros claims to have issued another letter dated November 23, 2005 notifying customers of a patch to stop storing track data. *See* Deposition Exhibit 28.
[28] Interview with Alan Mann June 22, 2010.

Micros that Cotton Patches' POS systems were adequately updated to avoid fines and comply with current industry requirements.[29] Following work by Micros to remediate the problem, Mr. Marshall viewed reports that appeared to confirm that masking was now occurring on internal Cotton Patch reporting.

40. On April 2, 2007 Micros authored another document addressed "Dear MICROS Customer" again with the IMPORTANT LEGAL NOTICE legend and reading in part: "It is imperative that you immediately upgrade your systems to versions that adhere to Visa's Payment Application Best Practices." *See* M000281. Based on my conversations with Cotton Patch employees, I understand that Cotton Patch did not receive this document prior to the CPP notice, nor did Micros adequately follow up with Cotton Patch regarding the March 2004 upgrade, the availability of RES 3.2 SP7 HF5, or the April 2007 document.

41. On or about June 15, 2007 Visa published a list of compliant payment applications that included Micros RES version 3.2 SP 7 HF5. The list indicated that this version of Micros RES, which Cotton Patch did not have at its Nacogdoches location, was compliant as of December 31, 2006. Again, Micros failed to communicate that to Cotton Patch.

42. Beginning August 17, 2007 Micros is aware that several Cotton Patch locations are non-compliant with some parts of the Fair and Accurate Credit Transaction Act ("FACTA") and PCI DSS. *See* M000299-300 (regarding the masking of certain sensitive card holder data and other PCI requirements including the encryption of sensitive CHD). In an email chain sent to Cotton Patch, it appears that Micros is

---

[29] Deposition of Larry Marshall at 214:3-215:18; Interview with Larry Marshall June 23, 2010; Plaintiff's Interrogatory Response 14 on pages 12-13.

communicating to Cotton Patch for the first time that full PCI compliance is also not available at several Cotton Patch locations, including Nacogdoches. *Id.*

43. Cotton Patch indicates that they do not recall receiving any of the Micros documents regarding compliance with PCI, and that even if Cotton Patch had received them, they would have asked Micros as their trusted vendor to address the issues. Indeed, when the compliance discussions occurred regarding FACTA requirements for masking of the full payment card number and expiration date on hard copy receipts, Cotton Patch sought and received assurance from Micros that all of the Micros POS systems in use at Cotton Patch's Nacogdoches restaurant met the prevailing industry security requirements in effect at the time.[30]

44. On or about August 23, 2007 Cotton Patch was alerted by RBS that common point of purchase analysis[31] by Visa and MasterCard (MC) had identified the Nacogdoches site as a potential common point of purchase for the compromise of CHD. In the Trustwave report regarding the security breach, it was noted that Cotton Patch did not comply with PCI DSS because there was, among other findings, a) full track data without encryption on the Micros POS system, b) default and or common or shared userids and passwords on PCAnywhere, c) no Internet firewall, and d) active Malicious Software (Malware) present on one or more Micros systems (likely due to out of date anti-malware controls).[32] *See* M000144-147. As shown in this report, Micros was in a position to know about and/or remedy all these issues before the alleged breach occurred.

---

[30] Interview with Alan Mann June 22, 2010; *See* also Deposition of Larry Marshall at 214:3-215:16.

[31] Common Point of Purchase (CPP) analysis is by definition, a statistical correlation of the last sets of valid transactions with a pattern of fraudulent transactions. It does not conclusively tie the fraud to the merchant, only a forensic analysis can potentially complete that tie. In the end, the Trustwave report was unable to determine if any card information specifically used in fraud was ex-filtrated from Cotton Patch. Trustwave indicated that the conditions existed for this to have happened.

[32] Each of the two latter conditions, no firewall and active Malware, almost certainly existed in 2006 when the server at Nacogdoches was physically replaced by Micros. I also understand that Micros installers were

45. Shortly after the breach notification, Mr. Marshall was informed by Micros that a patch existed that would have prevented the breach because it stored transaction data in a secure, encrypted Transaction Vault.[33]

E. The Trustwave Report on the Alleged Breach

46. I analyzed the report of Trustwave dated November 16, 2007. *See* M000140-164. I am familiar with the methodologies involved in developing such a report based on an investigation and examination of systems. In this report, Trustwave is unable to definitively establish that, for a variety of reasons, a breach did occur at the Cotton Patch Nacogdoches location, and if so, what information, if any, had been taken. However, Trustwave did identify a number of critical issues which likely may have resulted in a breach, and speculated about the potential for a breach. Importantly Trustwave stated:

- Default and/or Common userids and passwords were used in PCAnywhere; and
- Unencrypted, full magnetic stripe track and sensitive CHD data was found.

47. Micros was well aware of these specific vulnerabilities in the Micros system running at the Nacogdoches location which allowed the storage of unencrypted track data post-authorization. Micros was also well aware of the use of default and/or common userids and passwords for remote access of the Nacogdoches location over the Internet. *See, e.g.*, Deposition of Colin Sheppard at 70:24-71:4; Deposition of David Williams at 55:20-56:10. The Trustwave report confirms that the Nacogdoches location

---

trained to verify that up to date malware controls were present. *See* M000508; Deposition of Clayton Starkweather at 72:16-73:15.

[33] Interview with Larry Marshall on June 23, 2010.

was non-compliant with the then-applicable PCI DSS, PABP and other standards, which Micros was aware of well before the alleged breach. Despite this knowledge and its representations to Cotton Patch regarding the security and compliance of the Nacogdoches system, Micros failed to upgrade the Nacogdoches POS system or adequately notify Cotton Patch of these serious vulnerabilities.

48. I personally examined a forensic image of the Nacogdoches server provided by counsel. Among other things, my examination revealed the presence of full track data for what appear to be MasterCard (MC) accounts, and full unencrypted PAN information for what appear to be Visa, MC, American Express, and possibly other card brands. My examination is consistent with the observations of Sheppard.

IV. Opinions

49. Based on the analysis set forth above, the following conclusions are warranted:

- Micros controlled the proprietary POS software running at the Cotton Patch Nacogdoches location.
- Micros sold to Cotton Patch the POS equipment and ancillary software used by Cotton Patch at the Nacogdoches location.
- As a restaurant unfamiliar with the technology underlying proprietary POS systems such as that provided by Micros as well as applicable PCI and data security standards governing the operation of such systems, Cotton Patch lacked the knowledge, ability, experience or capacity to understand, identify or remediate the security vulnerabilities present in the proprietary Micros system.

- Micros directed Cotton Patch to "stay out" of the proprietary POS system, and Cotton Patch reasonably followed that direction.[34]
- Micros was aware of the PCI compliance status of its own products.
- Micros was aware of the PCI compliance status of its equipment installed at Cotton Patch sites, including at Nacogdoches.
- Micros represented to Cotton Patch that Micros would maintain the Micros POS system installed at the Cotton Patch Nacogdoches restaurant in a secure manner compliant with PCI and other relevant data security standards.
- As demonstrated by the Trustwave report and other documents produced by Micros and Cotton Patch, prior to the security breach detailed in the Trustwave report, the Micros POS system installed at the Cotton Patch Nacogdoches restaurant was not secure and did not comply with certain PCI security standards, including but not limited to requirements that POS systems not store full track data, not use vendor supplied, default, or common userids and passwords, and encrypt sensitive CHD.[35] Accordingly, Micros misrepresented to Cotton Patch that the POS system at the Nacogdoches restaurant was secure and compliant with prevailing industry standards, and failed to disclose that in fact they were non-compliant.
- Micros had an obligation and responsibility to Cotton Patch to maintain the Micros POS system installed at the Nacogdoches location in a PCI compliant manner. This obligation and responsibility arose as a result of Micros' oral representations to Cotton Patch, the parties' ongoing relationship, and through the unique knowledge that only Micros possessed about its application and the

[34] Interview with Alan Mann on June 22, 2010
[35] See Deposition of Colin Sheppard at 171:4-8.

PCI compliance status of the POS equipment and software at the Nacogdoches location.

- Micros never provided Cotton Patch with a secure configuration guide as required by Visa PABP and PA-DSS.[36]
- Micros repeatedly failed to adequately communicate or follow-up with Cotton Patch regarding the failure of the Micros system installed at the Cotton Patch Nacogdoches location to comply with PCI DSS and other relevant data security standards.

50. In my opinion, Micros, during the time leading up to the alleged breach, failed in its obligations to Cotton Patch as a payment application vendor and as the exclusive provider of POS products and services to Cotton Patch to provide a secure and PCI compliant POS system. This is evidenced by Micros' unique knowledge of non-compliance of certain of its RES equipment — including the equipment installed at Cotton Patch's Nacogdoches restaurant prior to the breach — with the then in-effect Visa Cardholder Information Security Program (CISP) and Payment Application Best Practices (PABP), and later with PCI DSS and PA-DSS, all of which set forth certain information security requirements to protect personal information and for the prevention of fraud. Payment application vendors, like Micros, are the developers and owners of the proprietary software in their payment applications. The source code and internal operation of the payment applications — including the storing of full magnetic track data, lack of encryption, and the use of default and/or common userids — are not generally available or known to merchants such as Cotton Patch. Payment application vendors like

[36] Interview with Alan Mann on June 22, 2010. See also, Plaintiff's Interrogatory Responses No. 12 at pages 11-12.

Micros directly obtain independent validation of compliance with PABP[37] and are encouraged to provide security configuration guidance, guidance that was never provided by Micros to Cotton Patch.

51. In my opinion, Cotton Patch clearly relied upon Micros, indeed necessarily had to rely upon Micros as the exclusive owner of the proprietary system, to provide a software product and ancillary products and services that complied with the obligations inherent with processing electronic payment card transactions.

52. In my opinion, Cotton Patch was reasonably diligent in relying upon Micros for compliance with the relevant requirements and for the security of card holder data at Cotton Patch. Moreover, Cotton Patch's reliance was reasonable given its relative lack of sophistication in the data security field, Micros' instructions that Cotton Patch was to "stay out" of the Micros system, the representations made by Micros regarding the security of the system, and the frequent maintenance performed by Micros on the POS system installed at the Nacogdoches restaurant.

53. In my opinion, Micros was in the best position to know, and in fact did know, that the version of Micros operating at the Cotton Patch Nacogdoches location prior to the alleged data security breach discussed in the Trustwave report was non-compliant with applicable PCI standards and vulnerable, and that Cotton Patch was relying upon Micros to maintain Cotton Patch's system in a reliable and secure manner, which Micros failed to do.

54. Based on my analysis of the Trustwave report and my experience in the data security industry, Micros' failings detailed above were the likely and foreseeable

---

[37] See, for example, http://usa.visa.com/download/merchants/validated_payment_applications.pdf?it=r|/merchants/risk_management/cisp_payment_applications.html|Validated%20Payment%20Applications

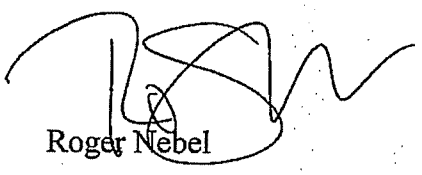
causes of the alleged security breach documented in the Trustwave report and directly led to fines assessed by the credit card industry. Moreover, absent these failings and the security vulnerabilities that they enabled, it is more likely than not that the security breach would not have occurred.

55. I have reviewed the expert report of James Walsh dated September 27, 2010. Among other things, I disagree with his conclusion that the security breach at Cotton Patch's Nacogdoches location "was the direct result of Cotton Patch's failures and negligence with respect to the security of their IT environment and systems." *See* Expert Report of James Walsh at III. B. 3. As demonstrated in my reports, Micros failed to provide a POS system that complied with, among other things, requirements for the elimination of full track data and encryption of sensitive CHD. These failings directly contributed to the fines assessed by the card brands and processors against Cotton Patch and could only have been remedied by Micros. Moreover my review of the materials provided in this case show that Micros failed to make an adequate effort to notify Cotton Patch of these issues, or to correct them prior to the CPP notice. In addition, Micros witnesses testified to using common, insecure userids and passwords to remotely access the Cotton Patch server at Nacogdoches. These failings of Micros cannot reasonably be blamed on Cotton Patch.

56. Furthermore, Micros' failure to adequately notify Cotton Patch prior to August 17, 2007 of the serious security vulnerabilities present in the Micros system installed at Cotton Patch's Nacogdoches restaurant is inexcusable in light of Micros' awareness of the vulnerabilities prior to that time, its awareness of relevant data security standards, and its representations to Cotton Patch concerning its responsibility to maintain a safe and secure POS system at, among others, the Cotton Patch Nacogdoches

location. A reasonable POS vendor would have taken many more steps and precautions to ensure that its customer, with whom it had an ongoing business relationship, was operating securely with respect to its use of the vendor-supplied POS equipment and software. Given the large fines and serious reputational repercussions that accompany data security breaches, this failing on the part of Micros gave rise to an extreme risk that Cotton Patch (and its customers) would suffer substantial financial harm.

57. This supplemental report is the result of new information provided to me since the original report. New information may come to light in the future and I reserve the right to further supplement my report as necessary.



Roger Nebel

Washington, DC

January 26, 2011